



## Highly Secured 3D Object Steganography Technique for Hiding Compressed Data

Aya AlKhamese<sup>1</sup>, Hewayda ElGawalby<sup>1,\*</sup>, Ahmad Eid<sup>1</sup>, Ibrahim Hanafy<sup>2</sup> and Wael Awad<sup>3</sup>

<sup>1</sup>Department of Physics and Engineering Mathematics, Faculty of Engineering, Port Said University, Port Said, Egypt

<sup>2</sup>Department of Mathematics and Computer Science, Faculty of Science, Port Said University, Port Said, Egypt

<sup>3</sup>Department of Computer Science, Faculty of Computers and Artificial Intelligence, Damietta University, Damietta, Egypt

\*Corresponding author: [aya.yakout@eng.psu.edu.eg](mailto:aya.yakout@eng.psu.edu.eg)

### ABSTRACT

Steganography is a technique that involves hiding a secret information within some objects such as images, audio, video, or 3D object, without leaving any noticeable or machine-detectable alterations. To ensure, more security and higher capacity, the steganographic techniques might include a data compression step for the secret information. In this paper, we propose a novel 3D steganographic technique, that enhancing both the security and the capacity of the 3D object used to hide the compressed secret information. For that purpose, we use the Gray code sequence to indicate the vertices of the 3D object used for concealing the compressed information; hence, we apply the LSB to embed the compressed information. The proposed steganographic technique has been evaluated through multiple metrics to assess its performance. These metrics include Embedding Capacity value, Mean Square Error Ratio, Peak Signal-to-Noise Ratio, and Normalized Correlation value. Experimental results illustrate that the proposed technique exhibits a high-level of security when compared to several existing techniques. Moreover, it provides robustness against noise, filtering and vertex reordering attacks.

### Key Words:

Data compression; Gray code; Gzip; LSB; PSNR; Secret key Steganography

## 1. INTRODUCTION

The importance of information security has grown with the increasing digitization of information. With a large quantity of confidential information being stored and transmitted electronically, organizations face new challenges in protecting this information from unauthorized access, theft, and attacks. To address these challenges, organizations have turned to a variety of information security technologies and practices, such as encryption and information hiding. Steganography is a method of

information hiding that involves concealing secret information within a cover object while it is being transmitted or stored. The goal of steganography is to make it ambitious for unauthorized parties to observe and extract hidden information. The cover object has several forms of digital representation, including text, audio, image, video, and 3D object. The embedding process may involve the use of a key called a secret key. The resulting stego object is the cover object with the hidden secret message [1, 2]. The increasing use of 3D objects in various applications, including gaming, virtual reality, and animation, has spurred the improvement of efficient techniques for hiding secret messages within 3D objects [3]. 3D steganographic techniques are designed to keep the secret message undetectable to unauthorized parties while offering increased capacity for message embedding. These techniques can be applied through one of three domains, namely geometrical, topological, and representational [4].

In this paper, we propose a novel 3D steganographic technique for concealing the message with a high level of security and capacity. The rearrangement of the vertices of the 3D object according to their distance of a certain vertex also increase the security of our technique. Two secret keys are used to enhance the security of the proposed technique. The Gray code sequence is utilized to disorder the 3D object vertices utilized in the embedding phase. The Gzip technique enhance the security and the capacity of the proposed technique. Our technique utilizes the LSB technique to conceal the binary representations of the compressed message.

Section 2 provides a brief overview of the LSB technique, the Gray code sequence, and data compression techniques. In Section 3, an analysis of some related studies that address the security aspects of the 3D object is discussed. Section 4 focuses on the contributions of the proposed technique. Section 5 delves into the main concepts and specifics of the proposed embedding and extraction algorithm. Section 6 evaluates performance using metrics and numerical analysis. Finally, Section 7 concludes this study by suggesting some future work.

## 2. Preliminary

This section provides an overview of the geometrical domain-based steganography, the LSB technique with its advantages, the Gray code sequence and its equation, and the definitions of data compression, including both lossless and lossy compression.

### 2.1. Geometrical Domain-based Steganography

The geometrical domain provides a high capacity for information hiding compared to the two other domains. 3D objects contain rich geometric information (such as vertices, triangles, and polygon mesh) that can be manipulated to conceal secret messages without causing noticeable changes to the cover object. As a result, many steganography techniques that use 3D objects have focused on exploiting the geometrical domain [5]. In the geometrical domain, the 3D steganographic techniques can be in the spatial domain or in the transform domain. Spatial domain techniques hide the message directly in the cover object, while frequency domain techniques use transformation functions to convert the cover object into coefficients, where the message is then hidden. The spatial domain is favored over the frequency domain because of its higher capacity and having simpler embedding and extraction algorithms [1].

#### 2.1.1. Least Significant Bit (LSB)

Least Significant Bit (LSB) embedding technique is a commonly utilized technique in spatial domain. The LSB technique requires substituting the least significant bits of one or more pixels in an object with the binary stream of the message. The modification in the brightness, contrast, or color intensity of pixels due to this substitution is negligible and cannot be perceived by the human eye. The substitution can be either successive or pseudo-random, where in successive substitution, each pixel is modified in the same order as the embedded bits, and in pseudo-random substitution. The order of substitution is determined using a pseudo-random number generator (such as Lucas sequence, triangle sequence, and Gray code sequence) [6].

### 2.1.2. Gray Code Sequence

Gray code sequence is a helpful tool in several applications and has earned a place as a fundamental concept in the computer science field and digital communications field. Two consecutive numbers in the Gray code sequence only differ by one digit, making it a very unique and efficient way of representing the binary data. Using the Gray code sequence, it can be done using only small changes between each number in the sequence, making it ideal for use in applications where the order of bits is important. The Gray code sequence is also used in error-correction algorithms, as it can detect single-bit errors in data transmission more easily than other binary numbering systems [7, 8].

The formula utilized to alter number  $B_0, B_1, B_2, \dots, B_n$  to its corresponding Gray code number  $G_0, G_1, G_2, \dots, G_n$  can be expressed as follows:

$$(1) \quad G_k = \begin{cases} B_k & \text{if } k = n \\ B_{k+1} \oplus B_k & \text{if } 1 \leq k \leq n-1 \end{cases}$$

The following equation is used to alter the Gray code number to an equivalent binary number:

$$(2) \quad B_k = \begin{cases} G_k & \text{if } k = n \\ B_{k+1} \oplus G_k & \text{if } 1 \leq k \leq n-1 \end{cases}$$

where  $\oplus$  operation is the bitwise (XOR) operation [9].

Table 1 demonstrates the relationship between decimal numbers, natural binary, Gray code binary, and the decimal of the Gray code sequence, as described in the example with  $N=3$ :

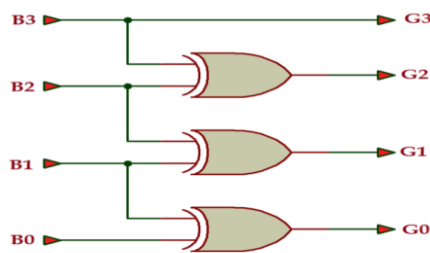


Figure 1. Conversion Process from Natural Binary to Gray Code Binary

**Table 1.** Representations of Numbers 0 Through 7: Decimal, Binary, Gray Code Binary, and Decimal of Gray

Decimal	0	1	2	3	4	5	6	7
Binary	0000	0001	0010	0011	0100	0101	0110	0111
Gray coded binary	0000	0001	0011	0010	0110	0111	0101	0100
Decimal of Gray	0	1	3	2	6	7	5	4

### 2.1.3. Data Compression

Data compression is utilized in minimizing the message size to find available space for the embedding process [10]. Classifying compression techniques can be performed by categorizing them based on the model used to identify the redundancy in the data. Lossless compression techniques and lossy compression techniques are the main groups of compression techniques. Lossless compression techniques maintain all the information present in the data, resulting in an identical reconstruction of the original data. On the other hand, lossy compression techniques discard some information in the original data, leading to a permanent loss of information. [11]. Gzip is a technique of lossless compression. It scans for repeating sequences in the data and replaces them with links to the first occurrence of the sequence [12].

Gzip is a popular compression technique due to its ability to provide high capacity, freedom from patent limitations, and ease of implementation [10]. The use of data compression in the proposed 3D steganographic technique increases the capacity of secret messages to be embedded in 3D objects. It also plays a role in data security by making it more difficult for unauthorized parties to access secret messages.

### 3. Related Work

P. Thiagarajan [14] has addressed 3D objects to embed large amounts of information. The binary stream if the message is embedded in the newly added positions after re-triangulating part of a triangle mesh. K. Anish [15] suggested a basic method for concealing data in a 3D geometrical domain. This approach involves altering the x-coordinate of the object to hide the secret bits. The decimal representation of the message is concealed in the modified x-coordinate value. S. Farrag [17] embedded the encrypted messages within a 3D object by altering the fourth and fifth decimal places of the vertices forming the polygons. The process of message hiding is accomplished by altering the decimal places to odd or even numbers depending on the information bit. A. Girdhar [22] modified the disparity between the vertices to conceal the message. A chaotic logistic map is utilized to choose the coordinates used for embedding. S. Farrag [13] has addressed an algorithm that traverses the mesh between neighboring vertices based on the shortest distances between them. The fourth or fifth decimal place after the decimal point of the vertices is changed to an even or odd number, depending on whether the binary bit to be embedded is 0 or 1. G. Mostafa [8] described a double layer algorithm for secure message embedding in 3D objects. The algorithm consists of a cryptography layer using either the Blowfish or AES-128 algorithm and a steganography layer utilizing the sequence of Gray code. By utilizing the Gray code sequence, the arrangement of the vertices is determined for concealing the secret messages. The message is subsequently embedded within the x, y, and z coordinates of vertices. S. Mukherjee et al [25] proposed a new 3D image steganography technique using VCI construction and bit shifting strategy. It has the capability of adjusting the embedding capacity with better visual quality. The advantages of this technique are higher embedding capacity, adjustable distortion, efficiency and robustness. S. Bandyopadhyay [26] encrypted the data using the AES technique for enhancing the protection. Next, depth first search, a geometric domain oriented steganography technique is utilized, in which triangular meshes' each vertex of several 3D images are subtly altered to hold the hidden data.

### 4. Contributions of The Proposed Technique

This section contains the main contributions of the proposed 3D steganographic technique (security, embedding capacity and robustness).

#### 4.1. Security

The proposed steganographic technique uses two secret keys to enhance privacy and security. The first key is used to rearrange the vertices of the 3D cover object, while the second key generates the Gray code sequence. Without knowing the first key, the hidden message cannot be extracted, as the 3D stego object vertices cannot be arranged to uncover the message. Without knowledge of the second secret key used to generate the Gray code sequence, the hidden message cannot be extracted. Mean Square Error Ratio (MSE), Peak Signal-to-Noise Ratio (PSNR), Histogram, and Normalized Correlation (NC) are used to evaluate the performance of the proposed technique. The Gray code sequence is utilized to enhance the security. It is used to specify the disorder of the vertices where the message is concealed.

#### 4.2. Capacity

The proposed technique also aims to increase the embedding capacity while preserving a high-quality 3D stego object. By compressing the message using the Gzip technique, the number of bits that must be concealed in the object is reduced, which in turn increases the hidden message security.

### 4.3. Robustness

The proposed technique was tested against common attacks such as noise, vertex reordering, smoothing, and similarity transforms to assess its efficiency and robustness.

## 5. The Proposed Technique

The proposed steganographic technique for 3D objects involves two phases: an embedding and an extraction phases. This technique enhances the security by utilizing the Gray code sequence and two secret keys and increases the embedding capacity through data compression.

### 5.1. The Proposed Embedding Phase

The proposed technique uses the data compression technique to effectively conceal a significant volume of data with a high level of security. Here, the Gzip compression technique is utilized to decrease the size of the secret message. Two stego keys are used in the proposed technique to enhance security. The Gray code sequence is utilized to conceal the compressed secret message. The 3D object vertices are reordered in ascending order of their distances from specific position.

#### 5.1.1. The Proposed Embedding Algorithm

The following algorithm outlines the steps involved in the embedding process of the proposed steganography technique:

- 1) Read 3D objects and obtain their vertices.
- 2) Reorder the vertices in ascending order according to their distances from specific position. This position is utilized to create the first stego key.
- 3) Create the first stego key utilizing binary representation of this position.
- 4) Convert these vertices to binary representation.
- 5) Embed the binary representation of the first stego key in the three least vertices of the z-coordinate.
- 6) Read the secret message.
- 7) Compress the message by the Gzip technique.
- 8) Convert the compressed message into its binary representation.
- 9) Generate the second stego key using the size of the compressed message binary representation to form the Gray code sequence.
- 10) Embed the binary representation of the second stego key in the three least vertices of the z-coordinate.
- 11) Generate Gray code sequence using the second stego key.
- 12) If the Gray code number is "0" or "1", one bit of the compressed message is to be concealed in the LSB of the vertex x-coordinate.
- 13) Otherwise, if the Gray code number is "2", two bits of compressed message is embedded in each LSB and its previous bit of x-coordinate
- 14) If the Gray code number is prim, a bit of compressed message is concealed only in the LSB of the x-coordinate
- 15) If the Gray code number is not prim and even, two bits of compressed message is concealed in each LSB and its previous bit of y-coordinate
- 16) If the Gray code number is odd and not prim, a bit of compressed message is concealed only in the LSB of the y-coordinate

### 5.2. The Proposed Extraction Phase

This phase involves the use of two secret keys to obtain the message. The first key is extracted from the last three vertices of the z-coordinate. This key is used to reorder the vertices of the cover object in ascending order according to their distances. The reordered vertices are then converted to binary representations. The second secret key is obtained from the last three vertices of the z-coordinate. This key is utilized to construct the Gray code sequence. The binary representation of the compressed message

is extracted from the ordered vertices. Convert the extracted binary representation to plain text. The plain text is then decompressed using the Gzip method to reveal the secret message.

### 5.2.1. The Proposed Extraction Algorithm

The following algorithm outlines the steps involved in the extraction algorithm of the proposed steganography technique:

- 1) Read the 3D object and obtain their vertices
- 2) Extract the first stego key from the three least vertices of the z-coordinate.
- 3) Reorder the vertices in an ascending order of their distances from specific position (first key).
- 4) Convert these vertices to binary representation.
- 5) Extract the second stego key from the three least vertices of the z-coordinate.
- 6) Generate the Gray code sequence using the second stego key.
- 7) If the Gray code number is “0” or “1”, extract the LSB of the x-coordinate at this index.
- 8) If the Gray code number is “2”, LSB and its previous bit of x-coordinate are obtained.
- 9) If the Gray code number is prim, the LSB of the x-coordinate is obtained.
- 10) If the Gray code number is not prim and even, LSB and its previous bit of the y-coordinate are obtained.
- 11) If the Gray code number is not prim and odd, the LSB of the y-coordinate is obtained.
- 12) Convert the extracted stream into an 8-bit binary representation and then to plain text.
- 13) Decompress the plain text using the Gzip method.

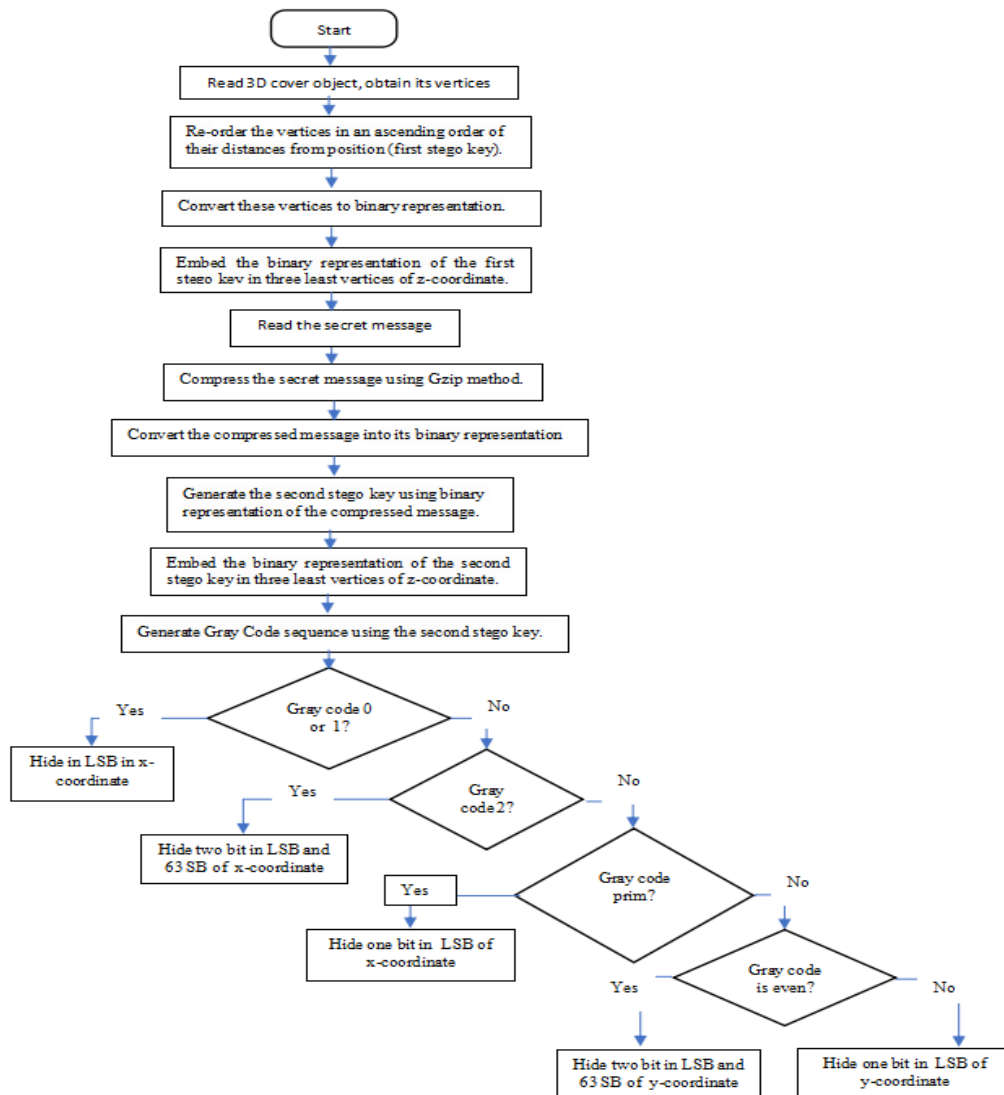


Figure 2. The Proposed Embedding Algorithm.

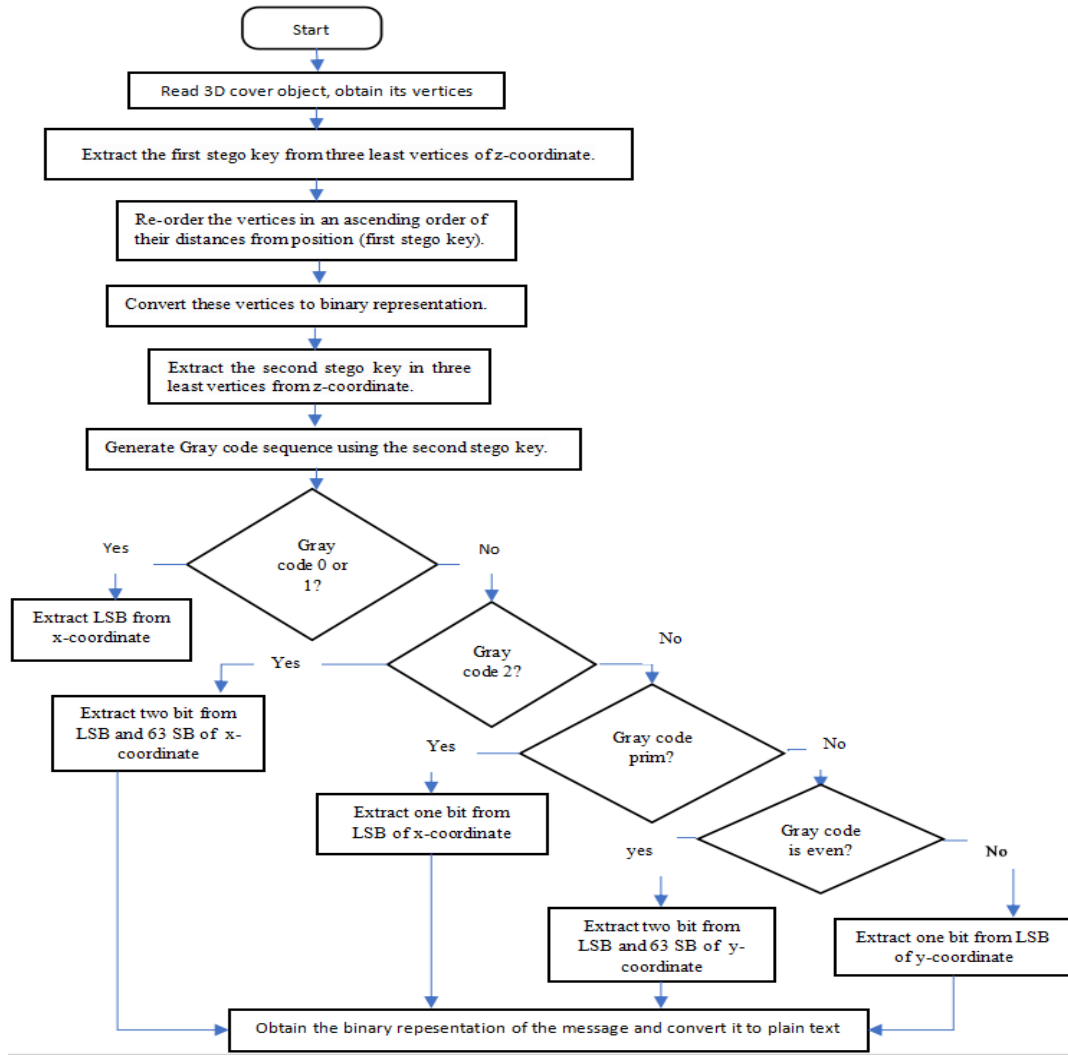


Figure 3. The Proposed Extraction Algorithm.

## 6. Performance Evaluation and Numerical Analysis

The proposed technique is implemented using Python on a machine running a 64-bit operating system that has Intel® Core(TM) i5-1135G7 2.40GHz CPU and 8.00 GB of RAM. In steganography, the capacity refers to how much secret messages can be hidden within a cover object, without the hidden messages being noticeable and without compromising the quality of the stego object. Embedding capacity (EC) and Embedding rate [ER] are used to evaluate the capacity of the proposed technique. EC is basically measures the number of bits concealed in a 3D object. ER is measured using bits per vertex (bpv), which is equal to the length of embedded bits dividing the amounts of vertices of the cover object. The value of ER can be calculated using equation (3).

$$ER = \frac{\text{The number of embedded bits}}{\text{The number of vertices in the 3D object}} \quad (3)$$

Security means the visible degradation in the cover object after hiding processing. The goal is to make the embedding process as unobtrusive as possible so that a human observer cannot detect any changes in the 3D stego object [2, 20]. Human Visual System (HVS), MSE, PSNR, NC, and histogram are utilized to evaluate the impedance of the proposed technique. These metrics identify how good the change is after the steganographic technique is applied to the 3D cover object. PSNR evaluate the visual quality of the 3D stego object, which is calculated using the equation 4.

$$PSNR = 20 \log_{10} \left( \frac{D_{\max}}{MSE} \right) \quad (4)$$

where  $D_{\max}$  is the diagonal distance of the smallest oriented cuboid bounding box of the 3D object. The role of robustness is really important in steganographic techniques. Robustness pertains to the capability of preserving the hidden secret message without any alteration or loss, even when the cover object undergoes specific changes. These changes encompass intentional or unintentional steganographic attacks or other processing operations, including transferring, noise, cropping, rotation, filtering, and so on [20]. The robustness of the proposed technique was tested by conducting typical attacks with varying parameters and evaluating the results using the NC value. The value of NC measures the similarity between the 3D stego object and the 3D attacked stego object to determine whether the message hidden in the 3D cover object has been preserved. If the value of the NC is 1, it indicates that the 3D stego object is totally resistant to these attacks [2]. The results of these experiments are presented in Tables 7 and 8.

The technique was tested using 3D objects (as shown in Table 2), such as "Bunny", "Armadillo" and "Elephant" which were obtained from both a 3D image database and the internet. The results of these evaluations provide insight into the effectiveness of the proposed technique in achieving its intended goals of hiding data in 3D cover objects with high security, hiding capacity, and robustness.

Table 2: Some of The Famous Experimental 3D Objects and Their Number of Vertices

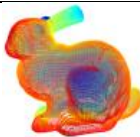


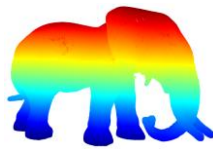
Name	3D object	Number of vertices
Bunny		35,947
Elephant		162,487
Armadillo		172,974

Figure 4 shows the initial stage of the analysis where a visual comparison is made between the cover and the stego objects. The histogram in Figures 5 and 6 confirm statistically that there are no noticeable differences that can be detected by HVS.



(a) 3D Cover Object



(b) 3D Stego Object

Figure 4. 3D Cover Object Versus 3D Stego Object with Maximum Embedding Rate



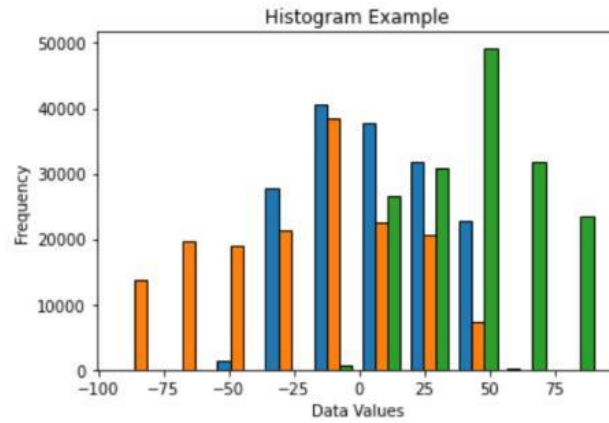


Figure 5. Histogram of 3D Cover Object “Elephant”

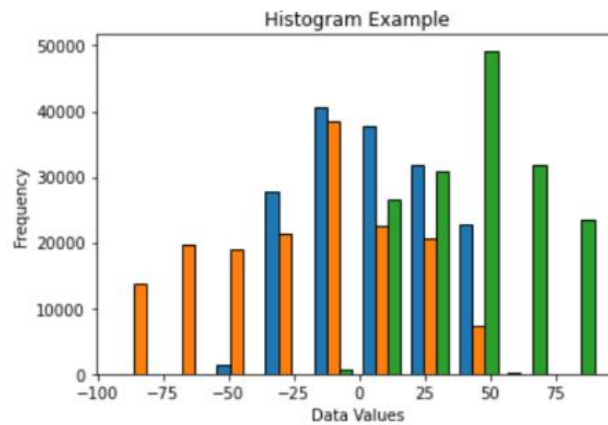


Figure 6. Histogram of 3D Stego Object “Elephant”

Table 3 shows the results of the performance evaluation metrics for multiple 3D objects, including EC, ER, MSE, PSNR, and NC. The results suggest that the proposed technique introduces minimal distortion, as evidenced by the MSE values being less than  $2 \times 10^{-30}$ . The values of PSNR for all objects are above 210 dB, indicating high-quality stego objects. The NC value is also 1 which indicates the higher

3D Object	Vertices	Maximum Embedding Capacity [EC]	ER	PSNR	MSE	NC
Bunny	35,947	51,944	1.445	213.157	$3.1432 \times 10^{-17}$	1.0
Elephant	162,487	184,176	1.133	345.287	$1.9245 \times 10^{-30}$	1.0
Armadillo	172,974	188,624	1.090	343.431	$2.9507 \times 10^{-30}$	1.0

quality of the proposed technique.

Table 3. Comparison Showing The Maximum Embedding Capacity, MSE, PSNR, and NC for Various 3D Objects

Table 4, a comparison is drawn between the suggested technique and other techniques within the geometry-based domain. Each of these techniques employs the spatial domain. They enable blind extraction of the hidden message from the stego object. Data compression is used only in the proposed technique and in technique [24] to enhance the security and the capacity of the message that can be concealed within the cover object.

Table 4. Comparison of Several Techniques in The 3D Geometrical Steganography-based Domain

Author	Algorithm	Embedding location	Data Compression	Blind
P. Thiagarajan [14]	Hiding after triangle mesh formation	Vertices	No	Yes
K. Anish [15]	Hiding in the x coordinate of a vertex	Vertices	No	Yes
A. Girdhar [22]	Hiding utilizing technique of difference shifting	Vertices	No	Yes
S. Farrag [17]	Hiding in the polygons forming	Polygon	No	Yes
G. Mostafa [8]	Hiding in the x, y, and z coordinates of a vertex using Gray code sequence	Vertices	No	Yes
A. Alkhamese [24]	Hiding in the x, y, and z coordinates of a vertex using three mathematical sequences	Vertices	Yes	Yes
S. Bandyopadhyay [26]	Hiding in each vertex of triangular meshes	Vertices	No	Yes
Proposed Technique	Hiding in the re-ordered x, and y coordinates of a vertex using Gray code sequence and data compression	Vertices	Yes	Yes

Table 5 shows a comparison between the proposed technique and other existing techniques [14, 23, 16, 8, 24] and [26]. This comparison indicates that our technique has a lower embedding capacity compared to [14, 16, 8, 24, 26]. The proposed technique is better at preserving the quality of 3D objects, as it has superior PSNR compared to other techniques. The proposed technique has lowest MSE compared to other techniques.

Table 5. Performance Assessment between Different Techniques

Author	3D Object	Maximum Embedding Capacity [bits]	PSNR	MSE
P. Thiagarajan [14]	Bunny	64,496	55.3442	0.18930
S. Elsherif [23]	Patient's head	1,792	53.1714	0.31329
W. Alexan [16]	CTEngine	295,680	62.66	0.03519
G. Mostafa [8]	Bunny	836,040	108.5830	$0.8678 \times 10^{-12}$
A. Alkhamese [24]	Bunny	164,216	146.792	$7.3442 \times 10^{-17}$
S. Bandyopadhyay [26]	Bunny	3,13,506	-	$0.165 \times 10^{-16}$
Proposed Technique	Bunny	51,944	213.157	$2.9507 \times 10^{-30}$

Table 6 demonstrates the MSE, and PSNR values for the "elephant" object with various embedding capacities (characters). The results indicate that the proposed technique can achieve high PSNR and low MSE. Figure 7 illustrates the visual impact of the embedding process with different values of EC and ER.

Table 6 The Results of The Embedding Capacity [Characters], EC, ER, and MSE for “Elephant” Object

Embedded characters	EC	ER	MSE	PSNR
6493	51,944	0.319	$1.761082 \times 10^{-30}$	345.673007
10566	84,528	0.520	$1.781920 \times 10^{-30}$	345.621921
16402	131,216	0.807	$1.831403 \times 10^{-30}$	345.502962
20300	162,400	0.999	$1.849738 \times 10^{-30}$	345.459699
23022	184,176	1.313	$1.884976 \times 10^{-30}$	345.377743

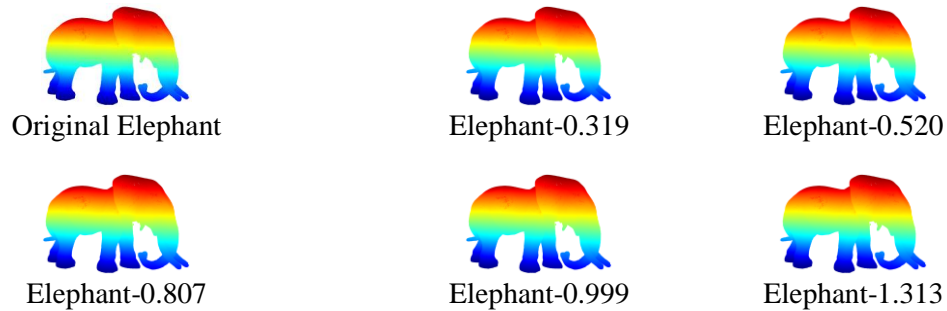


Figure 7. Visual Effect for The Cover- and The Stego-Objects with Different Embedding Rates

Tables 7 and 8 show the results of Normalized Correlation (NC) values against various attacks found in the literature, including Median filtering, Gaussian filtering, and Laplacian filtering. Table 8 shows the results of Normalized Correlation (NC) values against various noise attacks such as Gaussian, salt & pepper, and speckle. The proposed technique is susceptible to noise attacks, which can alter the vertex coordinates and cause incorrect data extraction.

Table 7 Normalized Correlation Values Against Various Attacks

Attacks		Bunny	Elephant
Median filtering	2X2	0.4248	0.6412
	3X3	0.2456	0.6002
Gaussian filtering	2X2	0.4983	0.9827
	3X3	0.2217	0.7168
Laplacian filtering		-0.6196	-0.8590

Table 8 Normalized correlation values against various noise attacks

Noise Attacks		Bunny	Elephant
Gaussian with variance	0.02	0.6252	0.9997
	0.05	0.6244	0.9987
Salt & Peeper		0.5124	1.0
Speckle		0.4213	0.6956

## 7. Conclusion and Future Work

The proposed technique aims to conceal substantial amount of secret information within 3D objects while preserving the object quality and security. This involves the incorporation of an additional security layer achieved by compressing the secret information using the Gzip technique. The empirical results showed that, the technique proposed in this paper represented a significant improvement over current algorithms in terms of security. Several metrics were used to assess the performance of the proposed

technique; including EC, MSE, PSNR, and NC. The experimental results indicated that the proposed technique has a higher security than that of similar techniques. The proposed technique has acceptable durability against attacks. Combination of geometrical based domain with representation based domain has raised the overall embedding capacity of the proposed technique. The topological characteristics of the 3D object can be utilized to enhance the security and the capacity of the proposed technique. The proposed techniques can be tested against other types of attacks.

## 8. References

- [1] A. Y. AlKhamese, W. R. Shabana, and I. M. Hanafy. "Data security in cloud computing using steganography: a review", 2019 International Conference on Innovative Trends in Computer Engineering (ITCE). IEEE, 2019, pp. 549-558, doi: 10.1109/ITCE.2019.8646434.
- [2] N. Kanzariya, D. Jadhav, G. Lakhani, U. Chauchan, and L. Gagani, "Coverless Information Hiding: A Review", Proceedings of International Conference on Computational Intelligence: ICCI 2021, Springer, 2022, pp. 109-135.
- [3] Y. Tsai, "An adaptive steganographic algorithm for 3D polygonal models using vertex decimation", Multimedia tools and applications, Springer, 2014, vol. 69, pp. 859-876, doi: 10.1007/s11042-012-1135-8.
- [4] S. Farrag and W. Alexan, "A high capacity geometrical domain based 3d image steganography scheme", International Conference on Advanced Communication Technologies and Networking (CommNet), IEEE, 2019, pp. 1-7, doi: 978-1-5386-8317-0/19/\$31.00.
- [5] S. Farrag and W. Alexan, "Secure 3d data hiding technique based on a mesh traversal algorithm", Multimedia Tools and Applications, Springer, 2020, vol. 79, pp. 29289-29303.
- [6] Despoina Giarimpampa, "Blind Image Steganalytic Optimization by using Machine Learning", PhD thesis, Halmstad University, 2018.
- [7] Wikipedia.URL: [https://en.wikipedia.org/wiki/Gray\\_code](https://en.wikipedia.org/wiki/Gray_code) (visited on 15/10/2022).
- [8] G. Mostafa, W. Alexan, "A robust high capacity Gray code-based double layer security scheme for secure data embedding in 3D objects", ITU Journal on Future and Evolving Technologies, vol. 3, pp.1, 2022, doi: 10.52953/UFGA9833.
- [9] C. C. Chen and C. C. Chang, "LSB-based steganography using reflected gray code", IEICE transactions on information and systems, The Institute of Electronics, Information and Communication Engineers, 2008, vol. 91, num. 4, pp. 1110-1116, doi: 10.1093/ietisy/e91-d.4.1110.
- [10] M. C. kasapba and W. Elmasry, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check", Springer, 2018, vol. 43, pp. 1-14.
- [11] K. Sayood, "Introduction to Data Compression", Fifth Edition, 2017.
- [12] A. M. Khadija, E. Sewesy, A. Abo and M. M. Hassan, "Secure Image Steganography Approach for Hiding Compressed Data", Soft Computing for Security Applications: Proceedings of ICSCS 2022, Springer, 2022, pp. 575-595.
- [13] S. Farrag, W. Alexan, "Secure 3D data hiding technique based on a mesh traversal algorithm", Multimedia Tools and Applications, Springer, vol.79, num.39, 2020.
- [14] P. Thiagarajan, V. Natarajan, G. Aghila, V. Prasanna Venkatesan, R. Anitha, "Pattern Based 3D Image Steganography", 3D Research, Springer, vol.4, pp.1-8, 2013.
- [15] K. Anish, N. Arpita, H. Nikhil, K. Sumant, S. Bhagya and S.D. Desai, "Intelligence System Security Based on 3-D Image", Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, Springer, pp.159-167, 2017.
- [16] W. Alexan, M. El Beheiry, and O. Gamal-Eldin. "A comparative study among different mathematical sequences in 3d image steganography.", International Journal of Computing and Digital Systems, University of Bahrain, vol.9, num.4, pp.545-552, 2020.

- [17] S. Farrag and W. Alexan, "A high capacity geometrical domain based 3d image steganography scheme". In 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), IEEE, pp.1-7, 2019.
- [18] S. Yasser, A. Hesham, M. Hassan and W. Alexan, "AES-Secured Bit-Cycling Steganography in Sliced 3D Images", 2020 International Conference on Innovative Trends in Communication and Computer Engineering (ITCE), IEEE, pp.227- 231,2020.
- [19] W. Alexan, M. H. Medhat, A. Hamza and H. Hussein, "Sequence-Based Bit-Cycling in Double Layer Message Security", IEEE, Advances in Wireless and Optical Communications, 2018.
- [20] U. A. Bhatti, L. Yuan, Z. Yu, J. Li, S. A. Nawaz, A. Mehmood and K. Zhang, "Hybrid watermarking algorithm using clifford algebra with Arnold scrambling and chaotic encryption", IEEE Access, 2020, vol. 8, pp. 76386-76398.
- [21] O. F. Abdel Wahab and Ashraf A.M. Khalaf and A. I. Hussein and Hesham F.A. Hamed."Hiding data using efficient combination of RSA cryptography, and compression steganography techniques", IEEE access, 2021, vol. 9, pp. 31805-31815.
- [22] A. Girdhar and V. Kumar, "A reversible and affine invariant 3D data hiding technique based on difference shifting and logistic map", Journal of Ambient Intelligence and Humanized Computing, Springer, vol.10, num.12, pp.4947-4961, 2019.
- [23] S. Elsherif, G. Mostafa, S. Farrag and W. Alexan, "Secure Message Embedding in 3D Images", 2019 international conference on Innovative Trends in Computer Engineering (ITCE), IEEE, pp.117-123, 2019.
- [24] A. AlKhamese, H. ElGawalby, A. Eid, I. Hanafy and W. Awad, "Double Layer Message Security For 3D Object Using Mathematical Sequences and Secret Keys," 2023 International Telecommunications Conference (ITC-Egypt), Alexandria, Egypt, 2023, pp. 607-614, doi: 10.1109/ITC-Egypt58155.2023.10206287.
- [25] S. Mukherjee, S. Sarkar, and S. Mukhopadhyay, "VCI Construction and Shifting Strategy Based Steganography for 3D Images", Computational Intelligence in Communications and Business Analytics. CICBA 2022. Communications in Computer and Information Science, vol 1579, pp. 210-219, Springer.
- [26] S.Bandyopadhyay, S. Sarkar, and S. Mukhopadhyay,"Hiding Secret Data Using AES Encryption and DFS Graph Traversal in 3D Images", 2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), IEEE, pp.1-4, 2023.